ENSIGN
INFOSECURITY

CONQUER
THE UNKNOWN

NIST CYBERSECURITY FRAMEWORK

Feedback to the NIST Cybersecurity Framework (CSF) 2.0

Prepared for:
NIST

Date:
4 March 2023

Prepared by
Ensign Consulting

Ensign InfoSecurity
30A Kallang Place, #08-01, S(339213)
[redacted]
Web : www.ensigninfosecurity.com

Table of Contents

1. About Ensign

Ensign InfoSecurity is the largest pure-play end-to-end cybersecurity service provider in Asia. Headquartered in Singapore, Ensign offers bespoke solutions and services to address their clients' cybersecurity needs. Ensign's core competencies are in the provision of cybersecurity advisory and assurance services, architecture design and systems integration services, and managed security services for advanced threat detection, threat hunting, and incident response. Underpinning these competencies is inhouse research and development in cybersecurity. Ensign has more than two decades of proven track record as a trusted and relevant service provider, serving clients from the public and private sectors in the Asia Pacific region.

The following input is prepared by Ensign Consulting, who provides cybersecurity advisory and assurance services to our client.

2. Ensign Consulting's Context of Adopting NIST Cybersecurity Framework (CSF)

Ensign Consulting Team leverages the NIST CSF to advise our clients on their cybersecurity posture. The NIST CSF is the primary reference framework for Ensign Cybersecurity Maturity Framework and maturity assessments, where we determine our client's sophistication in understanding and implementation of cybersecurity and cybersecurity controls. After the maturity assessments, we devise improvement programs for clients referencing the NIST CSF. In addition to maturity programs, NIST CSF is a supplementary framework for other assessments, where other frameworks are dictated by client's scope of work.

3. Feedback to NIST CSF 2.0

1. CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications.

1.1. Change the CSF's title and text to reflect its intended use by all organisations.

Ensign has no comment on this proposed change.

1.2. Scope the CSF to ensure it benefits organizations regardless of sector, type, or size.

Ensign proposes that NIST CSF 2.0 should not have sector-specific requirements or controls. Instead, the interpretation of the NIST CSF should be calibrated by associated threat environments and needs to be accompanied by threat analysis. This will benefit organisations by having visibility over all threat vectors that they are susceptible to, regardless of sector, type, or size.

In addition, as organisations may operate across several sectors, scoping of the CSF as proposed may causing confusion and challenges in achieving an appropriate level of maturity.

1.3. Increase international collaboration and engagement.

Ensign supports this proposed change. As Ensign operates in various countries, Ensign shares the URLS for the following relevant prevailing regulations in these countries for NIST's consideration :

No.	Documents	URL
1	*Singapore Personal Data Protection Act (PDPA) 2012*	https://sso.agc.gov.sg/Act/PDPA2012
2	*Malaysia Personal Data Protection Act (PDPA) 2010*	https://www.pdp.gov.my/jpdpv2/assets/2019/09/Communications-Sector-PDPA-COP.pdf
3	*Korea Personal Information Protection Act (PIPA) 2011*	https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3
4	*Hong Kong Personal Data (Privacy) Ordinance (PDPO)*	https://www.elegislation.gov.hk/hk/cap486
5	*Cybersecurity Codes of Practice (CCoP) 2.0 by Cyber Security Agency (Singapore)*	https://www.csa.gov.sg/docs/default-source/csa/documents/legislation/ccop_second-edition.pdf?sfvrsn=b2ab666a_0

2. CSF 2.0 will remain a framework, providing context and connections to existing standards and resources.

2.1. Retain CSF's current level of detail.

Ensign believes that the current level of detail is sufficiently brief and broad to allow for interpretation of the level of implementation based on the subcategories. However, if the intent is to progress towards a clearer definition for measurement, then the level of detail may have to be increased to prevent inconsistent measurements.

2.2. Relate the CSF clearly to other NIST frameworks.

Since the release of NIST CSF version 1.1, many cybersecurity concepts have been placed under the spotlight. NIST has developed a series of papers to guide the discussion for some of them, namely:

- Secure Software Development (SP 800-218)
- Zero Trust Architecture (SP 800-207)

- IoT Cybersecurity (NISTIR 8259 Series, SP 800-213)
- Cloud Security (SP 800-210)
- Cyber Supply Chain Risk Management (SP 800-161)
- Risk Management Framework (SP 800-37)
- Privacy Framework

In addition, the following topic has not received additional guidelines since NIST CSF version 1.1, but merits an update:

- OT Cybersecurity (SP 800-82)

Given that the vision for NIST CSF is to be the overarching framework for cybersecurity controls, organisations should be able to understand how to achieve specific cybersecurity objectives such as cloud security or IoT security in alignment with the outcomes described by NIST CSF. As a result, ***we recommend the inclusion of bidirectional guidance and references between these specific frameworks and NIST CSF.***

2.3. Leverage Cybersecurity and Privacy Reference Tool for online CSF 2.0 Core

Ensign would like to suggest that the mappings should be in machine readable format (e.g. XML, JSON, etc.) to allow the ease of data ingestion for any future use using tools.

2.4. Use updatable, online Informative References

Ensign agrees with the Online Informative References Program (OLIR) approach. We also suggest that a registered panel of contributors be established to vet and manage the contributions. This panel will then act as a jury panel to rectify and validate the contribution before the information is made available to the public.

In reference to the mapping, Ensign would also like to suggest that the mappings should be in machine readable format (XML, JSON, etc.). This allows the ease of data ingestion for any future use using tools.

2.5. Use Informative References to provide more guidance to implement the CSF.

Ensign provides its existing mapping of the CSF to SP800-53 controls with their respective maturity tiering to aid the public in understanding the maximum maturity that a CSF subcategory can achieve through various states of implementation of the associated SP800-53 controls. Please refer to provided document "NIST CSF Mapping to SP800-53 with maturity tiers", slides 1 – 6.

2.6. Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices.

Ensign agrees with this proposed change. Technology and vendor relevance may change with time and is a dimension that is best left outside of the CSF.

3. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation.

3.1. Add implementation examples for CSF Subcategories

Ensign shares its interpretation of the CSF Subcategories Implementation tiers to guide organisations in their journey of implementing the CSF within their organisation by working towards the outcome that is defined for their targeted implementation tier. Please refer to

[redacted]

provided document "NIST CSF Mapping to SP800-53 with maturity tiers", slides 7 - 8 for a sample definition for ID.AM.

3.2. Develop a CSF Profile template.

Ensign performs threat research on the threat landscape relevant to an organisation or group of organisations leveraging the MITRE ATT&CK framework. Furthermore, we leverage the ATT&CK to NIST SP 800-53 mapping to determine the appropriate target state calibrated by benchmark data and threat intelligence analysis.

3.3. Improve the CSF website to highlight implementation resources.

Ensign would like to share a success story of a Cybersecurity Maturity Study that was successively conducted for a client who is a Financial Services and Insurance Services. Our study is conducted based of the client's cybersecurity operations against our Cybersecurity Maturity Framework (CSMF) which is based on NIST Cybersecurity Framework.

Background

The client is a general insurance group in Asia. They aspired to be a reputable insurance provider in the region, enabled by a robust and leading cybersecurity posture. The initial maturity study was conducted in 2019 and a recurring study took place in 2021 to understand their intermediate state since 2019.

2019 Maturity Study

The client engaged Ensign to conduct a cybersecurity maturity study to help them understand their cybersecurity posture across the group.

The results of the maturity study (using a scoring scheme from 0 to 4) for the five (5) functional domains in 2019 were:

No.	***Domains***	***Assessment 1 Maturity***	***Assessment 1 Target Maturity***
1	*IDENTIFY (ID)*	*2.3*	*3.0*
2	*PROTECT (PR)*	*2.1*	*2.7*
3	*DETECT (DE)*	*1.6*	*3.0*
4	*RESPOND (RS)*	*2.2*	*2.6*
5	*RECOVER (RC)*	*2.1*	*2.3*

A total of thirteen (13) key initiatives were proposed across three (3) years for implementation, below were a few initiatives:

1. *Developing centralised Cybersecurity Governance*
2. *Implementing Continuous Security Monitoring*
3. *Implementing Cyber Threat Intelligence Capabilities*

2021 Maturity Study

The client re-engaged Ensign for the maturity study to understand their current cybersecurity maturity and to understand their progression since the study in 2019. Since 2019, a few initiatives have kicked-off. Thus, resulting in an increase in the current maturity results Highlighted in red are the results where material improvements were observed. You may also note that the Target Maturity in Assessment 2 are also different from that of Assessment 1 as a fresh threat analysis was performed to determine the Target Maturity.

No.	***Domains***	***Assessment 2 Maturity***	***Assessment 2 Target Maturity***
1	*IDENTIFY (ID)*	*2.3*	*2.9*
2	*PROTECT (PR)*	*2.5*	*2.9*
3	*DETECT (DE)*	*2.4*	*2.9*
4	*RESPOND (RS)*	*2.5*	*2.8*
5	*RECOVER (RC)*	*2.6*	*2.8*

4. CSF 2.0 will emphasize the importance of cybersecurity governance.

4.1. Add a new Govern Function

Ensign believes that adding this function may help to consolidate common governance topics which today cuts across the existing five functions.

4.2. Improve discussion of relationship to risk management

Current risk management processes involve identifying, assessing and prioritising risks based on the impact the risks have against the organisation. While risk to impact approach is widely used, Ensign proposes to include threat as part of risk management process, making it a threat to risk analysis approach.

Enhancement to the risk management process can be done by first performing a threat analysis and aligning them to a set of relevant key risk indicators. This allows us to identify risks that are relevant to the organisation before determining the residual risks after consideration of mitigation actions and controls.

5. CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (C-SCRM)

5.1. Expand coverage of supply chain

With reference to expanding C-SCRM in the ID.SC category in the Identify function, Ensign would like to propose to include Software Bill of Materials (SBOM) in the ID.SC category as well. By including SBOM, organisations can gain a better understanding and manage risks associated with software used by third-party vendors and suppliers.

Example of control: "SBOMs from the organisation's third-party vendors and suppliers are collected and maintained".

6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment.

    6.1. Clarify how leveraging the CSF can support the measurement and assessment of cybersecurity programs.

    As shared in the examples by Ensign, we believe that the CSF is a useful framework to measure and assess organisations for their broad positions in achieving maturity in cybersecurity governance and operations.

    6.2. Provide examples of measurement and assessment using the CSF

    Ensign uses the existing mapping of SP800-53 controls with maturity tiers to the relevant CSF subcategories to measure and assess an organisation's cybersecurity maturity. Please refer to NIST CSF Mapping to SP800-53 with maturity tiers, slide 9.

    6.3. Update the NIST Performance Measurement Guide for Information Security

    Ensign agrees that having a performance measurement guide would assist in helping organisations understand where they are in the capabilities.

    6.4. Provide additional guidance on Framework Implementation Tiers

    Refer to Ensign's response in 2.5.